## REMARKS

The Final Office Action of April 14, 2004 has been received and its contents carefully reviewed. Applicant acknowledges with appreciation Examiner's withdrawal of the prior objections to the Specification and the Title as filed December 12, 2003. Claims 1, 2, and 4-13 are pending in the present application.

Claims 1, 2, and 4-13 stand rejected under 35 § 112, first paragraph, as failing to comply with the enablement requirement. In particular, the Examiner asserts that the step of "generating a transformation key from the grantor's decryption key, the grantee's encryption key and other data which is data file independent" is not enabled by the cited portions of the specification. In response, in addition to the previously cited portions of the Specification, the above elements of the independent claims are clearly supported, for example, by FIG. 11 (e.g., step 1122) and discussion thereof in the Specification on page 36, line 19 to page 37, line 9 (emphasis added):

> Referring now to Figure 11, the scheme is set up the same way as a standard 20 ElGamal scheme (see Figure 6, described above). In addition, a symmetric, private-key encryption scheme is selected (step 1110). Its encryption function is $m$ |—> $E_K(m)$ and decryption function is $m$ |—> $E_K(m)$, where $K$ is some private key.
>
> To encrypt a document $m$, owner $A$ first chooses a uniformly random number $k \in Z^*_{p-1}$ (step 1112) and calculates a session key $K = g^k \pmod p$ (step 1114). The encrypted document $(r, s)$ is then calculated as follows:
>
> $$r = E_K(m) \text{ and } s = K^a \pmod p.$$
>
> (step 1116), where $a$ is A's private key. A keeps the pair $(s, k)$ private.
>
> Upon request from a recipient $B$ for the encrypted document $(r, s)$, $A$ first obtains $B$'s authentic public key $\beta$ (step 1118) and retrieves $k$ from the pair $(s, k)$ (step 1120). **$A$ then computes $\pi_B = \beta^k s^{-1} \pmod p$ (step 1122), where $s^{-1}$ is the inverse of $s$ modulo $p$, as the proxy key for $B$.**
>
> The document is then transformed by computing $s' = s\pi_B \pmod p$ (step 1124); the pair $(r, s')$ represents the transformed document customized for $B$.
>
> To decrypt the customized document $(r, s')$ and retrieve the original document $m$, $B$ first recovers the session key by calculating $K = s^{,b-1} \pmod p$ (step 1126), where $b^{-1}$ is the inverse of $b$ modulo $p-1$. Then the document itself is decrypted by calculating $m = D_K(r)$ (step 1128).

Accordingly, as recited in claim 1 (emphasis added), and as supported by the previously cited portions of the Specification, and FIG. 11 (e.g., step 1122) and discussion thereof in the Specification on page 36, line 19 to page 37, line 9:

> A method for protecting a data file on a computer system, comprising the steps of:
>
> providing a grantee's [$B$] encryption key [$\beta$], a grantee's [$B$] decryption key [$b$], a grantor's [$A$] encryption key [$\alpha$], and a grantor's [$A$] decryption key [$a$];
>
> using asymmetric encryption, encrypting the data file [$m$] using the grantor's [$A$] encryption key [$\alpha$] to create an encrypted data file [$r$];
>
> **generating a transformation key [$\pi$] from the grantor's [$A$] decryption key [$a$], the grantee's [$B$] encryption key [$\beta$] and other data which is data file independent [$k$];**
>
> transforming the encrypted data file [$r$] with the transformation key [$\pi$] to generate a transformed encrypted data file [$r, s'$] wherein the transforming of the encrypted data file [$r$] does not reveal the data file [$m$] during the process of transforming;
>
> providing the transformed encrypted data file [$r, s'$] to the grantee [$B$]; and
>
> decrypting the transformed encrypted file [$r, s'$] by the grantee [$B$] with the grantee's decryption key [$b$];
>
> wherein the transformation key [$\pi$] does not allow the grantee [$B$] to determine the grantor's [$A$] decryption key [$a$].

In a similar manner, independent claim 4 is clearly supported, for example, by the previously cited portions of the Specification, and FIG. 11 and discussion thereof in the Specification on page 36, line 19 to page 37, line 9. Accordingly, independent claims 1 and 4, and claims dependent therefrom, are in compliance with 35 U.S.C. § 112 and no further rejection on such basis is anticipated. If, however, the Examiner should disagree, the Examiner is invited to contact the undersigned, who will be happy to work with the Examiner in a joint effort to derive a mutually satisfactory solution.

In addition, the Specification at page 36, lines 3-8, has been amended to correct discovered informalities and so as to be consistent with the drawings and remaining portions of the Specification. No new matter is introduced. See in particular FIG. 11, step 1122, and Specification, page 36, line 26, in which $\pi$ is dependent on $\beta$ and $s$, and $s$ is dependent on $a$. Accordingly, $\pi$ is dependent on $\beta$ and $a$ (not α), which is reflected in the amended Specification. Also see, e.g., Specification, , FIGs. 8-11, elements 816, 916, 1116, 1016, and 1216, and the discussion thereof, and p. 21, lines 10-14 and 22-30, p. 22, lines 18-21, p. 27, lines 6-10, p. 28, lines 1-8 and 18-20, p. 29, lines 1-4, p.

31, lines 9-11 and 26-30, p. 32, lines 26-28, and p. 36, line 23 to p. 37, line 2.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. However, if the Examiner deems that any issue remains after considering this response, he is invited to call the undersigned to expedite the prosecution and work out any such issue by telephone.

Respectfully submitted,

Carlos R. Villamar
Reg. No. 43,224

NIXON PEABODY LLP
401 9th Street, NW
Washington, DC 20004
(202) 585-8000